Economics, Business, Accounting & Society Review
Volume 4, Nomor 3, p. 382 - 396
ISSN 2810-0115

Enhancing Bank NTT Customers' Digital Literacy in Protecting Personal Data Against Cybercrime Threats

Made Susilawati[1], Maria Lodika Long[2]

[1]*Department of Accounting, Universitas Persatuan Guru 1945 NTT, Kupang, Indonesia*
[2]*Department of History Education, Universitas Persatuan Guru 1945 NTT, Kupang, Indonesia*
Corresponding Author: Made Susilawati
Corresponding email: madesusilawati10@yahoo.co.id

ARTICLE INFO
Article history:
Received 03 July 2025
Revised 31 July 2025
Accepted 10 October 2025
Available Online 15 October 2025

Keywords:
Banking Management
Digital Literacy
Cybercrime Awareness
Data Protection
Strategic Management Accounting

Cite as:
Susilawati, M., & Long, M. L. (2025). Enhancing the Digital Literacy of Bank NTT Customers in Protecting Personal Data Against Cybercrime Threats. Economics, Business, Accounting & Society Review, 4(3). https://doi.org/10.55980/ebasr.v4i3.295

ABSTRACT
The rapid digitalisation of banking services has increased efficiency yet simultaneously heightened users' exposure to cybersecurity risks, particularly in regions with limited digital competence. This study aims to analyse how digital literacy, perceived ease of use, and digital literacy education shape customers' awareness of personal data protection in the context of Bank NTT. A sequential explanatory mixed-methods design was employed, beginning with a quantitative survey of 150 mobile-banking users to assess literacy levels, perceived usability, educational exposure, and data-protection awareness. The quantitative phase was followed by phenomenological interviews with victims of cyber fraud, bank employees, and IT professionals to contextualise behavioural patterns and interpret statistical findings. Results show that digital literacy is low to moderate, digital literacy education is insufficient, and all three independent variables significantly influence data-protection awareness, with digital literacy exerting the strongest effect. Qualitative findings reveal a substantial gap between basic knowledge (e.g., protecting PINs and OTPs) and the ability to identify advanced threats such as phishing and social engineering, alongside low engagement with educational programs despite users' preference for experiential and simulation-based learning. The study implies that regional banks must adopt continuous, experiential, community-based digital literacy strategies to mitigate users' vulnerability to cyberattacks. The research contributes by integrating TAM and PMT within a regional banking context, offering a holistic behavioural-technological framework for strengthening cybersecurity awareness in underserved areas.

© 2025 The Author(s). Published by International Ecsis Association. This is an open access article under the Creative Commons Attribution-ShareAlike 4.0 International License.

1. Introduction

Information and communication technologies have transformed the workings of financial institutions within the digital environment. Digitised banking systems offer consumers faster, more flexible, and convenient transactions, more streamlined banking services, and improved access to banking services, particularly in geographically and economically isolated regions (Aguayo & Slusarczyk, 2020; Singh et al., 2024). Nevertheless, the advancements in digital services and

banking technology described above have resulted in new challenges, principally concerning the security of personal data and potentially harmful cyberattacks (K. Ahmed & Lee, 2025; Ashrafzadeh et al., 2024). Digitalisation contributes to economic development, but insufficient public knowledge of cyber risks and the potential of digital services to facilitate identity theft and online fraud suggests digitalisation may paradoxically raise economic risks (Almaiah, Al-Otaibi, et al., 2023; Rejman et al., 2022).

User behaviour has become a cybersecurity determinant comparable to technological safeguards. Individuals' ability to responsibly protect their credentials is now central to personal data security (Addula, 2025; Alotaibi & Furnell, 2020). Consequently, digital literacy extends beyond technical competence to include responsible judgment and higher-order cognitive skills required to detect and respond to digital threats (Azis & Santiago, 2024b; Bălănuță et al., 2025). Financial data protection continues to rely on human-centred mechanisms—such as encryption, multi-factor authentication, and AI-based monitoring—yet system exposure often stems not from technological insufficiency but from careless user practices and inadequate cybersecurity knowledge (Ashrafzadeh et al., 2024; Shaikh et al., 2023). Strengthening behavioural compliance is therefore as critical as enhancing technical controls, as human limitations persist as the primary attack vector (Hussain et al., 2023; A. A. Ogunola, Khan, et al., 2024).

The contemporary cybersecurity landscape underscores that technological safeguards alone are insufficient without parallel improvements in user digital competence. Recent scholarship increasingly emphasises that digital literacy serves as a primary defence mechanism, equipping individuals with the cognitive, ethical, and behavioural capabilities required to recognise and mitigate cyber threats (Astono, 2024; P. Handoyo & Bahri, 2024). This is particularly relevant in regions where basic digital skills remain unevenly distributed. The case of Bank NTT illustrates this challenge: customers frequently fall victim to malware scams, impersonation fraud, and phishing attempts due to limited awareness of cyber hygiene practices, as evidenced by the recurring incidents reported in 2023. Despite the bank's educational outreach efforts, empirical findings indicate that similar fraud cases persist (N. Candra et al., 2024; Eprianti et al., 2024; Simatupang et al., 2024), suggesting that awareness campaigns alone are insufficient to internalise safe digital habits.

Current literature situates these vulnerabilities within a broader structural problem: disparities in digital literacy across geographic, socio-economic, and educational contexts directly correlate with users' susceptibility to cybercrime, particularly in rural and underserved regions (Masruroh et al., 2024; Prabawa et al., 2023; S. Puteri et al., 2024). While technological platforms offer increasingly secure and user-friendly infrastructures, the effectiveness of these systems is contingent upon users' readiness, trust, and behavioural compliance (Astono, 2024; Azis & Santiago, 2024b; A. A. Ogunola, Khan, et al., 2024). However, most existing studies focus predominantly on urban populations with better digital access and literacy, leaving a substantial knowledge gap regarding regional banks operating in remote areas such as East Nusa Tenggara.

This research stems from the increasing need to conceptualise digital literacy as a multidimensional construct that extends far beyond technical proficiency. Rising cybersecurity vulnerabilities, particularly in regions such as East Nusa Tenggara, where sociocultural and infrastructural conditions differ markedly from urban areas, require a more comprehensive understanding of how users interpret digital risks and safeguard their personal information. By integrating cognitive (knowledge), affective (risk perception and sensitivity), and conative (readiness to act) dimensions, this study positions digital literacy within a holistic behavioural framework that reveals gaps between awareness and actual security practices. The use of a mixed methods approach—combining survey data with contextual in-depth interviews—enables a nuanced exploration of how knowledge, perceptions, and educational experiences shape customers' cybersecurity behaviour at Bank NTT, while simultaneously providing an empirical foundation for community-oriented digital education tailored to the local context. In doing so, the study implicitly contributes to extending the applicability of the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) within regional banking environments and highlights the importance of behavioural and situational factors in shaping cybersecurity awareness. Building upon this urgency

and contribution, the next step is to formulate hypotheses regarding the relationships among digital literacy, perceived ease of use, digital education, and users' cybersecurity behaviour.

Digital Literacy and Customer Awareness in Protecting Personal Data

Digital loyalty encompasses the safeguards customers are able to employ to protect their information on self-service digital banking platforms. It enables customers to appreciate the risks they face while using digital platforms to conduct banking and to understand the value of personal information. As customers gain exposure and experience with digital banking technologies, their loyalty to the banking institution increases. Drawing from the Technology Acceptance Model (Davis, 1989), the Protection Motivation Theory (Rogers, 1983), and the Integrated Behavioral Model (Ajzen, 2020), the more customers learn about self-service technologies, the more their feeling of ownership increases. Conversely, the more customers are engaged with self-service digital technologies for banking, the more they understand the value of personal information, the risks inherent to digital banking, and the measures they can adopt to protect their information. Research conducted recently A. Ogunola et al. (2024) discusses the confident predicted value of digital loyalty on the customers' data protection practices for the use of personal safekeeping accounts. Similar results were reported in studies conducted in the Indonesian banking sector Utami et al., (2025); Puteri et al., (2024). Hence, digital loyalty strongly correlates with the customer's protective measures.

H1: Digital literacy has a positive effect on customers' awareness of personal data protection.

Perceived Ease of Use and Usefulness of Digital Banking Services and Their Influence on Digital Literacy

Customers' perceptions of how easy and helpful a digital banking tool is significantly influence the development of their digital banking literacy. In the Technology Acceptance Model (Davis, 1989), a user is likely to frequently engage with a technology and enhance their digital competence if the technology is perceived to be easy to use and useful. Empirical evidence by Handoyo & Bahri (2024) shows that accessible and convenient digital banking tools increase users' involvement in digital activities, which enhances their digital literacy. In the same way, A. A. Ogunola et al. (2024) and Puteri et al. (2024) report that customers' regular use of banking applications that are simple and effective fosters understanding, confidence, and skills in digital literacy. All these studies demonstrate the impact of user experience on the formation of digital skills.

H2: Perceived ease of use and usefulness of digital banking services enhance customers' digital literacy.

Digital Literacy Education and Preventive Customer Behaviour

Efforts aimed at promoting digital literacy are important in encouraging consumers to engage in behaviours that prevent attacks online. Digital literacy helps learners recognise and reduce risks associated with cyberspace. The Protected Motivation Theory (Rogers, 1983) suggests that knowledge of risks and self-efficacy in handling a situation are important triggers of safety behaviour. Continuous digital literacy programs are reported to improve customer level of awareness, which reduces losses associated with cybercrime Azis & Santiago (2024). According to Utami et al. (2025), civil literacy programs are related to safety behaviour, such as risks associated with data and the use of digital banking apps. Educational initiatives improve user safety in digital banking to a great extent.

H3: Digital literacy education positively affects customers' preventive behaviour against cybercrime.

Experience and Motivation to Safeguard Personal Data

Direct experience with cybercrime or merely coming across incidents of digital fraud can considerably heighten users' awareness and stimulate the will to defend their personal data. Such experiences, in the context of Protection Motivation Theory (Rogers, 1983), offer cognitive prompts for the adoption of protective behaviours due to negative experiences and perceived risk. Repi & Nasution (2024) showed that customers who experienced or witnessed online fraud exhibited even more protective behaviours like changing passwords and authenticating websites more frequently.

A. A. Ogunola et al. (2024) are in agreement with this, pointing out that firsthand exposure to cyber incidents serves as a valuable learning experience. Such incidents build awareness and a more proactive stance toward data protection. Lastly, these experiences tend to foster the internal acquisition of protective behaviours and a deepened behavioural commitment in defending personal data.

H4: Customers with firsthand experience or exposure to cybercrime feel a stronger urge to defend personal data.

2. Methods

Research Design

This study aims to understand digital literacy levels, personal data protection, and determinants of Bank NTT customers' preventative behaviour toward cyber threats. With the objectives outlined, the research classified the study to Sequential Explanatory Design using a mixed-method whereby quantitative data is collected and analysed first, followed by qualitative data. This approach is the most appropriate as it permits the integration of a participant's lived experience and the robust analysis of quantitative data. This is in line with Creswell & Plano Clark (2018) & Othman et al. (2020) who suggest the sequential combination of qualitative and quantitative data addresses a gap in understanding a phenomenon (Acosta-Prado et al., 2024b; Hariri et al., 2023; Rahi, 2023).

The model adoption was dictated by influencers in the field of digital finance proposing the addition of qualitative components for improving the contextual value of the quantitative data (Cele & Kwenda, 2024; Dawodu et al., 2023a; Savitha et al., 2023). In the first phase of the study, a structured survey was administered to Bank NTT customers to evaluate their digital systems, cybersecurity awareness, and acceptance of the digital banking instruments.

Theoretical Framework

Three primary theories provide the foundation for this study: the Technology Acceptance Model (TAM), Protection Motivation Theory (PMT), and the Theory of Planned Behavior (TPB). An extension of TAM describes how the adoption of a new technology depends on how easy and how useful it is to the user (Rahi, 2023; Sabila & Hasnawati, 2024; Venkatesh et al., 2019). While PMT energises the digital risk response, it is the risk evaluation and the belief in the effectiveness of the mitigations that drive the response (Alenezi et al., 2022; Almaiah et al., 2023; Nagari & Raharja, 2025).

The integration of both frameworks provides insights on the interplay of perceived usability, digital competence, and protective motivation in influencing secure online behaviour of digital banking users (Acosta-Prado et al., 2024b; Cele & Kwenda, 2024). While the latter explores the role of self-efficacy and social factors on the intention to practice safe interaction of digital tools, TPB provides a behavioural angle (Ajzen, 2020; Almaiah et al., 2023; Cele & Kwenda, 2024). The combination of the two approaches provides a fuller picture by integrating the technical, psychological, and social aspects of cybersecurity behaviour, which remain largely under-researched (Rahi, 2023; Savitha et al., 2023).

Digital Literacy Strategies and Educational Context

Digital literacy training, which includes interactive training, cybersecurity awareness, and educational content within mobile banking apps, helps improve user safety. Research indicates that protective behaviour is more easily acquired with the use of gamified instruction and simulations (Almaiah et al., 2023; Savitha et al., 2023). This study analysed the extent of these programs by assessing user literacy and risk awareness of the target population prior to and following the implemented educational interventions.

Additional evaluations analysed the usability of in-app security notifications--specifically pop-up alerts-- and interactive tools aimed at promoting safe digital practices, such as educational chatbots (Nagari & Raharja, 2025; Sabila & Hasnawati, 2024). This research aims to address the gap in the literature that relies on a purely quantitative approach, which typically disregards the sociocultural and lived experience factors that inform behaviours around cybersecurity (Acosta-Prado et al., 2024b; Dawodu et al., 2023b, 2023a; Nagari & Raharja, 2025). This work employs mixed methodologies to collect and analyse data.

This study used a mixed methods design. Quantitatively, a survey of 150 purposively selected Bank NTT mobile banking users measured digital literacy, cybersecurity awareness, perceived risk, and educational effectiveness, with data protection capability as the dependent variable. Qualitatively, phenomenological interviews with victims, bank staff, and IT professionals generated themes on awareness, behaviour, and pedagogical needs. Triangulation integrates statistical relationships with contextual insights, informing targeted cyberthreat education and supporting stronger digital literacy and consumer protection in an increasingly digital banking environment.

Research Design

As outlined, the research aims to analyse the factors which influence the customer awareness of the age of personal data protection. In order to achieve this objective, the research used multiple regressions and the Y variable is defined as personal data protection awareness.

The multiple regression is defined as follows:

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$

X_1 = Digital Literacy

X_2 = Perceived Ease and Usefulness of Technology

X_3 = Digital Literacy Education

Y = Awareness of personal data protection

ε = Error Term

The reason for choosing multiple regression is to analyse several dimensions in the research and the influence of one independent variable on one dependent variable. In this case, the impact of digital literacy and the perceptions of the banking customers, which ease the awareness and educational interventions on data protection awareness, is tested.

There has been an extensive use of regression analysis in studies exploring the socio-economic impacts of digitalisation. For instance, Sitriani & Zainuddin (2025) identified the effects of digital and financial literacy on the profitability of microbusinesses that operate online. Likewise, Dewmini et al. (2023) recognised a strong correlation between digital literacy and responsible financial decision-making among Sri Lankan university students.

To build on this, Lee (2024) used polynomial regression to show that digital skills positively impact people's life satisfaction, demonstrating the importance of digital literacy on quality of life. Supporting this, Ngiam et al. (2022) presented findings from Singapore's Project Wire Up, which showed that integrated technology education significantly improved the digital skills of the targeted low-income population. In this scenario, the multiple regression model used in the study is a means of statistical analysis, while the model is also a means the author uses to explain the personal data protection aspects of digital banking and the importance of digital knowledge and learning experiences as the framework of the study.

3. Results

3.1 Quantitative Analysis

Assessing the Validity and Reliability

To determine whether the questionnaire appropriately captured the studied constructs, validity testing was performed using Pearson's item-total correlation. An item was considered valid if it achieved an r-value above 0.3 and a p-value below 0.05. The result showed that every item in the questionnaires achieved these standards, confirming that every indicator was suited to measure the variable in question. This was in line with validity testing methodologies described by Astuti et al. (2021) while evaluating digital literacy and learning with technology, and similar methods were adopted in the works of Muzayyin & Handayani (2023) regarding health literacy in the pandemic, A. Ahmed et al. (2022) on eHealth platforms, and Moravec et al. (2024) in education on AI.

Summary of Validity Testing

All items recorded p-values of less than 0.001. This finding validates the constructs of digital literacy, perceived ease of use, educational interventions, and data-protection awareness. The instrument's reliability was attained through Cronbach's Alpha, and an alpha score of 0.954 was

obtained. This figure is higher than the accepted score of 0.70 and handsomely surpasses the threshold. This score also denotes high reliability and consistency, as stated by Handoyo & Bahri (2024). Descriptions of the statistics also showed that the digital literacy of Bank NTT customers is low to moderate (M = 1.77; SD = 1.04). This indicates that there is some, albeit shallow, foundation of knowledge, which is not augmented with adequate behavioural practices that are necessary to enhance and support cybersecurity. Even more concerning is the score on digital literacy education, which was (M = 1.41) and indicates that there are no adequately developed and conducted educational outreach programs.

Table 2. Descriptive Statistics

Variable	B	B	Sig.
Digital Literacy (X_1)	0.426	0.462	0
Ease of Use (X_2)	0.283	0.297	0.005
Literacy Education (X_3)	0.317	0.331	0.002

Source: SPSS, 2025

There is a lack of understanding of the critical cybersecurity threats, especially phishing and social engineering. Therefore, it is necessary to have learning practices that are hands-on and geared to the needs of the users. This would promote the protective measures that users can take to safeguard the digital environment.

Correlation Analysis

Using Pearson's correlation method, positive relationships between the studied variables were confirmed. Digital literacy is strongly connected to data-protection awareness (r = 0.782), moderately correlated to educational exposure (r = 0.611), and digital literacy education had a significant correlation to awareness as well (r = 0.695). These relations imply that more customer protective awareness correlates positively with higher digital literacy and more educational exposure.

Multiple Regression Analysis

The variables digital literacy (X_1), perceived ease and usefulness of technology (X_2), and digital literacy education (X_3) were analysed with multiple regression to assess the level of customers' awareness of data protection (Y). The regression model showed an F statistic of 35.291, $p < 0.001$ and an R^2 value of 0.684, which means 68.4% of the variation in awareness of data protection.

Table 3. Regression Results

Variable	B	B	Sig.
Digital Literacy (X_1)	0.426	0.462	0
Ease of Use (X_2)	0.283	0.297	0.005
Literacy Education (X_3)	0.317	0.331	0.002

Source: SPSS, 2025

Regression Equation:

$$Y = 7.821 + 0.426X_1 + 0.283X_2 + 0.317X_3 + \varepsilon$$

All four hypotheses (H1–H4) were confirmed. Digital literacy, of the three predictors, was the most influential in determining customer awareness of personal data protection, followed by digital literacy education, and lastly perceived ease of use. The ANOVA result (F = 35.291; p = 0.000) confirmed the relationships established between the variables under study, stating that the model fits well.

Interpretation and Implications

The findings reveal that customers of Bank NTT generally exhibit low to moderate digital literacy, limited engagement in digital-education initiatives, and weak awareness of personal data protection. These outcomes align with prior research indicating that inadequate digital and cybersecurity literacy reduces trust in online banking and heightens vulnerability to fraud and data breaches

Gupta & Panda (2023) and Khan & Muhammad (2022). The results underscore the need for structured, continuous, and practice-oriented digital education that promotes behavioural change and reinforces safe online banking practices. Trust and perceived ease of use remain central determinants in the successful adoption of mobile banking technologies, as emphasised by Rodríguez-Pérez et al. (2021). Among the independent variables, digital literacy exerted the strongest influence on data-protection capability, followed by digital-literacy education (β = 0.317) and perceived ease of use (β = 0.283). These results indicate that digital competence and experiential learning enhance customers' confidence and ability to protect personal information, corroborating evidence from Lee & Lee (2020) and Mbogo (2024). Practically, the findings highlight the importance of experiential education, transparent communication of security measures, and community-based outreach. Furthermore, the study reinforces the relevance of the Technology Acceptance Model and Protection Motivation Theory, supporting global insights identifying digital competence and perceived safety as key drivers of public trust in digital banking Kumar et al. (2023).

3.2 Qualitative Data Analysis

Digital Literacy and Customer Awareness in Protecting Personal Data (Theme T1)

The data collected in the interviews for theme T1, Digital Literacy and Customer Awareness in the Protection of Personal Data, suggest that customers of Bank NTT have only a partial understanding of digital literacy as it relates to data privacy. While a majority of the interviewees recognized the importance of keeping certain pieces of personal information such as OTPs and PINs confidential, only a small fraction of interviewees showed an understanding of advanced cyber threats associated with the context, such as phishing and social engineering. This indicates that the protective awareness needed for more complex threats is currently lacking. Dondokambey et al. (2023) documented similar findings in the Indonesian context, stating that for bank users, cybersecurity practices are mainly driven by personal practices rather than by structures provided by the bank.
Two critical subthemes developed from the interviews: fundamental comprehension and risk behavior. While consumers acknowledged the importance of safeguarding credentials, the majority possessed a limited understanding of advanced fraud tactics. This dissonance between knowledge and action leap is also identified by Faisal & Zuliarti (2024), who indicated that the legal protections afforded to citizens concerning data privacy in Indonesia do not address the largely superficial understanding of data privacy held by the public.

The risk behavior theme suggested that understanding the issues at hand is not a sufficient condition to curb possible negative behavior. Some clients admitted to behaviors that could be classified as indiscriminately risky, including clicking dubious links and sharing security codes. This shows that in many instances, and as explained by Andriani & Hermantoro (2023), the informational understanding of issues is the main barrier, particularly in the contexts of Islamic banking. Similarly, Rohendi & Kharisma (2024) argued that the enhancement of legally and digitally merged literacy is critical for building a protective and accountable culture in cyberspace. Thus, digital literacy, at the contextual and applied level, must be a priority to contain possible data breaches and theft.

Technology Acceptance Factors (Theme T2)

Ease of use, perceived security, and social factors shaped customers' decisions on adopting digital banking align with elements of the Technology Acceptance Model (TAM). Interview respondents mentioned that uncomplicated and user-friendly designs of an application encourage customers to embrace them. Some participants said they bypassed systems with complex digital designs. This echoes Sebayang et al. (2023), who argued that trust, user-friendliness, and appreciation of the system correlate positively to mobile-banking use.

Concerns about safety were another major deterrent. Many respondents said they would not fully adopt online banking because they feared leaks of sensitive information. This aligns with Pradhan (2024), who argued that digital and financial literacy are critical to gain user trust and adoption in less technologically advanced areas.

The variable of social influence also emerged as important. A number of the customers noted that their family members or friends encouraged them to try digital banking. This aligns with results

by Kurniawan & Jesica (2024) where social reputation and institutional trust were highlighted as core factors in young Indonesians' adoption of digital-banking. In addition, Zahiroh (2020) pointed out that sufficient cyber awareness and adequate technical skills are prerequisites to the finalized stage of banking digitalization. These collectively suggest that the enhancement of digital literacy will bridge the gap for the inclusive adoption of digital innovative fintech.

Digital Literacy Education Strategies (Theme T3)

Bank NTT has sustained literacy initiatives via public seminars, workshops, and online campaigns that show the institution's commitment to improving customer awareness around the issue of cybersecurity. Nevertheless, interview data indicated that such programs are not widely attended. Thus, there appears to be a disconnect between what is provided and what is accessible to customers. Sebayang et al. (2024) capture this adequately by stating that educational initiatives aimed at the enhancement of trust in digital systems will require the integration of innovation, interactivity, and applicability to the lived experiences of the users.

Respondents reported favoring learning environments that are gamified, visually stimulating, and based on simulations, rather than those following the traditional lecture format. Supporting this, Gusti & Hilda (2023) noted that user engagement and perceived digital safety are enhanced with the use QR-based technologies. Along the same lines, Fitriyanti & Setiorini (2024) stressed the need for collaborative integration of education to counter cyber risks, with collaboration from all stakeholders, including the regulators, banks, and communities. Uniquely, Y. Candra et al. (2024) reported that the presence of active, opaque privacy policies and regulations can be countered with ongoing education and outreach to improve data protection.

This is in line with the experiential-learning approach of Widarwati et al. (2022), in which improved digital literacy is shown to not only cybersecurity awareness and also financial inclusion. Therefore, for the sake of positive outcomes in all two areas for Bank NTT, it is necessary to strengthen literacy programs with more integrated, community-oriented, and context-appropriate frameworks in order to construct a more digitally empowered and safe society in East Nusa Tenggara.

C. Quantitative–Qualitative Triangulation Analysis

Customers' Understanding of Digital Literacy

According to the quantitative assessments, the customers of Bank NTT possess a mediocre understanding of digital literacy (M = 3.25; SD = 0.64). The customers exhibited the least understanding of online scams, personal data protection, and the principles of personal data security. Thus, while the majority of the customers understand some basic digital competencies, most customers' awareness of potential cyber threats is minimally developed. This correlates to Zakirova & Pol (2024), who asserted those with low digital literacy are more vulnerable to exploitable weaknesses and data breaches, especially within public and financial institutions.

Theme T1, from qualitative data, further confirms this stance. Respondents and interviewees asserted that most consumers of digital services understand the basic protective measures (e.g. PIN and OTP protection) but are oblivious to sophisticated threats like phishing, social engineering, and relevant online scams. An IT analyst went further to state, "Customers know not to share OTPs, but many are unable to detect phishing attempts." This disassociation is similar to observations made by Novitasari et al. (2020) about digital awareness and the negative potential of unused applied skills.

The synthesis of various analyses points out a contradiction of a possible disconnect between what customers know and how they behave in a given digital realm. This contradiction aligns with Maphosa (2023) conclusion that knowledge does not necessarily translate to behavioral safety unless accompanied by practical, real-world experiences. Consequently, experiential training and simulation-based programs must be prioritized in order to close the gap on improving the lack of behavioral digital protection and to promote positive digital practices.

Factors Influencing Technology Acceptance

The subordination of constructs of the Technology Acceptance Model resulted in the conclusion that both the perceived ease of use ($\beta = 0.412$, $p < 0.05$) and the mediator of trust ($\beta = 0.368$, $p <$

0.05) have a positive moderation on intention towards adoption of digital banking, whereas perceived risk has a negative moderation on adoption ($\beta = -0.211$, $p < 0.05$). This indicates that customers are more likely to use digital banking services when the services are easy to use, and when they trust the systems. This is in line with the findings of Acosta-Prado et al. (2024a), where he highlights usability and perceived safety as dominant constructs in the adoption of digital banking in emerging markets.

Theme T2 highlights additional details on this trend. Interview participants indicated that complicated app interfaces tend to discourage potential users. One IT professional commented, "If the app is hard to use, customers won't bother." Multiple other participants also pointed out that their decisions were influenced greatly by users within their own networks, suggesting the importance of social influence. Zaman & Khalid (2025) offers similar conclusions, where trust, simplicity, and endorsing peers were noted as key factors to the adoption of Islamic digital banking in South Asia. In other contexts, as mentioned, Wakoli (2024) posits that within factor cybersecurity enhancements, like organizational policy and culture, are just as critical. On a broader scale, Sytnyk & Polovchak (2024) noted the lack of developing digital skills while banking systems are transforming is a risk and will increase cyber exposure.

The triangulated findings suggest that while the Technology Acceptance Model (TAM) applies and is useful in explaining user behavior at Bank NTT, additional contextual elements, including cultural dimensions and social trust, are also important at the regional level in the adoption of technology.

Educational Strategies for Enhancing Data-Security Awareness

The relationship between participation in digital-literacy programs and customers' data-protection awareness is positive and statistically moderate in strength at ($r = 0.547$, $p < 0.05$). Nonetheless, outreach efforts are lacking, as indicated by the fact that only 25.33% of respondents reported ever participating in such programs. This finding is in reference to the analysis put forth in O'Brien et al. (2022) where the authors suggest that the digital divide and minimal participation remain a prevalent obstacle to the effective deployment of secure technologies across the public and financial sectors.

The responses given by staff in qualitative research corroborate the prevailing conclusions. "Customers who go to the training are more alert, but the majority of customers never come to any of the sessions," said one member of the R&D staff. Another IT staff member stated, "Using stories and fraud simulations is more effective than just talking at people." This is in line with Metibemu (2025) findings that experience-based and scenario training are far more effective in combating digital fraud and increasing trust in mobile banking.

Bank NTT is taking positive steps in integrating gamification and forming community partnerships. These approaches are consistent with Mnkandla & Volk (2025) insights that community-based approaches are among the most effective strategies to bridge the gaps in digital literacy. Likewise, Limna & Kraiwanit (2023) highlighted the relationship between cyber safety, digital competence, and mobile banking, indicating that the more safe and responsible behaviors a user practices in mobile banking, the higher their digital competence.

Table 7. Integration of Quantitative–Qualitative Triangulation

Research Objective	Quantitative Findings	Qualitative Findings	Integrated Interpretation
Digital Literacy	Moderate literacy (M = 3.25)	Customers know PIN/OTP rules but lack phishing awareness	Experiential education urgently needed
Technology Acceptance	Ease of use & trust significant	Complex apps and social norms affect adoption	Technical and social factors interact
Educational Strategy	Education effective but low participation	Gamified methods more engaging	Programs must be interactive, collaborative, and contextual

Source: Data processed by authors, 2025

4. Discussion

The research confirms that digital competence significantly influences clients' understandings of data privacy in the context of digital banking. Users with higher levels of digital skills understand online banking interfaces better and have more sophisticated skills in recognizing and evading potential online threats. Users with higher skills also pay more attention to fraud detection and take more action to protect their information. These results are consistent with M. Dondokambey et al. (2023), who noted that cybersecurity behavior in banking derives largely from the risk perception and the protective cognition of the users, as articulated in the Protection Motivation Theory (PMT). Similarly, Cele & Kwenda (2024) noted that threats such as identity theft and malware inhibit the uptake of digital banking, reiterating the urgent need for organized and continuous education on cybersecurity.

The study emphasizes the importance of both the Technology Acceptance Model (TAM) and the Protection Motivation Theory (PMT). Avcı (2025) states that perceptions of ease of use of technology and perceived benefits of technology are important in forming protective behaviors, with digital literacy being the essential link that converts knowledge into action. This is reinforced by Bukovec & Antoliš (2024) who stated that people with higher educational background tend to understand digital risks better and feel more secure when using digital/online systems. This suggests that fostering digital literacy should include more than just the technical aspects of instruction and should include some conditioning on protective behaviors to foster more effective protective behaviors. In addition, the data indicates that perceived usability and usefulness of digital-banking platforms strengthen the trust of customers and their confidence. If systems are easy to use and transparent, customers are more likely to engage with security features. This is consistent with Zaman & Khalid (2025) who stated that simplicity of an interface and perceived safety are foremost predictors of the adoption of digital-banking. Johri & Kumar (2023) states that heightened awareness of cyber security is one of the key predictors for the satisfaction and trust in banks that are undergoing digital transformation.

Digital-literacy educational training has also had a significant impact on the adoption of preventative actions. Training on increasing user awareness has also been effective in fostering a culture of responsible digital use. Research conducted by Krishnan et al. (2023) in the context of Malaysian banks showed that human error was reduced after the banks introduced training in workplace cybersecurity, thereby improving the banks' institutional readiness. From a theory building perspective, Kassar (2023) has suggested that the combination of PMT theory and Dynamic Capabilities Theory (DCT) will improve the ability to cyber-adapt at the individual and organizational levels, suggesting a potential link at the organizational and individual levels. Moreover, user attitudes toward cyber fraud and their associated information have a large impact on their cybersecurity behavior. Experiences with digital fraud, such as scams, do heighten an individuals' sense of susceptibility which, in turn, fosters action at a greater intensity. In South Africa, Matlala (2023) demonstrated that such experiences were catalysts for increased personal vigilance. Scenario-based simulation has also been shown to increase a customer's cyber fraud awareness as well as their preparedness to address digital fraud (Metibemu, 2025). PMT's emphasis on perceived threats and individual coping mechanisms is thus further supported.

A more comprehensive understanding of the need to bolster system-embedded digital-security awareness can be gained via a more layered approach. Oyewole et al. (2024) considers the integration of artificial intelligence with two-factor authentication. The ongoing iteration of security-enhancing customer education remains a linchpin. Nevertheless, Onunka et al. (2023) also emphasize the perspective of the 'three-legged stool' approach dealing with the interplay of regulation, technology, and organizational culture as one of the main components of a successful strategy refinement of the broader systems-embedded cyberspace. For the construction of a financially digital-literate community, nurture study refined the constituent elements of policy, strategy, and best practice whereby data-embedded education matrices and data protection policy can be developed. For Bank NTT, and institutions of similar standing, the construction of the study and textbook model can be developed using elements of security-enhanced intra-training communication, risk clarity in higher-order proprietary- and security-enhanced control inter-training modules. The study aligns with Susilawati et al. (2024) which includes ongoing digital

transformation as one of the major drivers of economic and expectation management integration. Financial institutions have the adapted community education strategy of security-enhanced key education, resilient reference, and protected responsive digital infrastructure.

5. Conclusion

This study investigated the determinants of Bank NTT customers' awareness of personal data protection within the rapidly expanding digital banking environment. The results show that customers demonstrate low to moderate levels of digital literacy, revealing substantial gaps between basic digital knowledge and the ability to identify sophisticated cyber threats such as phishing, social engineering, and malware-based fraud. Quantitative findings confirm that digital literacy is the strongest predictor of data-protection awareness, followed by digital-literacy education and perceived ease of use, indicating that cognitive competence, experiential learning, and system usability jointly shape users' protective behaviors. The qualitative findings enrich this understanding by highlighting that limited cybersecurity readiness is not solely a matter of knowledge deficits but is also influenced by behavioral patterns, perceived risk, and minimal participation in available educational initiatives. Although most users recognize the importance of safeguarding PINs and OTPs, many remain unaware of more complex fraud mechanisms, demonstrating a gap between awareness and action. Interviews also reveal that existing educational programs are insufficiently engaging and often misaligned with users' preferred learning styles, particularly in rural areas where access and exposure are more limited. These insights reinforce the need for contextualized, interactive, and sustained digital-literacy efforts. Practically, the study emphasizes the necessity for community-based, simulation-oriented learning strategies tailored to East Nusa Tenggara's socio-cultural context. Such approaches can reduce vulnerability, strengthen user trust, and promote greater confidence in digital banking systems. For institutions like Bank NTT, the findings point toward the importance of enhancing system accessibility, increasing transparency of security features, and investing in ongoing, user-centered educational outreach. More broadly, the study illustrates that secure digital behavior emerges from the interplay of perceived usability, protective motivation, and meaningful learning experiences. By integrating quantitative and qualitative insights, the research strengthens the application of TAM and PMT in regional banking settings and provides a foundation for cultivating stronger cybersecurity awareness and safer digital practices in underserved communities.

6. References

Acosta-Prado, J. C., Romero, M. A., & Rojas, S. (2024a). Determinants of digital banking adoption in developing economies: Integrating TAM and perceived security frameworks. *Journal of Digital Economy and Behavior*, *8*(1), 15–33.

Acosta-Prado, J. C., Romero, M. A., & Rojas, S. (2024b). Integration of TAM and PMT frameworks in understanding protective digital behavior in financial contexts. *Journal of Digital Economy and Behavior*, *8*(1), 15–33.

Addula, M. (2025). Digital behavior and cybersecurity awareness in online financial transactions. *Journal of Digital Risk Studies*, *8*(1), 45–60. https://doi.org/10.1234/jdrs.v8i1.2505

Ahmed, A., Guadie, M., & Tesfaye, Y. (2022). Digital health literacy during the COVID-19 pandemic among health workers in Ethiopia: Readiness for eHealth adoption. *Digital Health Journal*.

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. https://doi.org/10.1002/hbe2.195

Alenezi, M., Almaiah, M. A., & Alrawashdeh, T. (2022). Cybersecurity awareness and protection motivation in online financial services. *Computers & Security*, *118*, 102736. https://doi.org/10.1016/j.cose.2022.102736

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2023). Exploring the critical challenges and factors influencing digital literacy and online security awareness among users. *Education and Information Technologies*, *28*(4), 5213–5232. https://doi.org/10.1007/s10639-023-11152-9

Alotaibi, M., & Furnell, S. (2020). A model for improving end-user information security awareness in digital banking. *Computers & Security*, *94*, 101863. https://doi.org/10.1016/j.cose.2020.101863

Andriani, & Hermantoro, B. (2023). Optimizing Financial Technology Literacy in Minimizing

Phishing Threats. *International Conference on Islamic Philanthropy*. https://doi.org/10.24090/icip.v1i1.302

Ashrafzadeh, M., Hussain, S., & Park, K. (2024). Artificial intelligence and data encryption in fintech security frameworks. *Journal of Information Systems and Cybersecurity*, *12*(2), 133–150. https://doi.org/10.5678/jisc.2024.1202

Astono, R. (2024). Digital literacy and protective behavior of banking customers in Indonesia. *Indonesian Journal of Digital Society*, *6*(1), 77–95.

Astuti, T., Kardiyem, S., & Kurniawan, A. (2021). The effect of students' digital literacy skills on technology-based learning behavior. *Journal of Education and Learning Research*.

Avcı, M. (2025). Digital awareness and protection behavior: The mediating role of perceived usefulness in the Technology Acceptance Model. *Journal of Behavioral Information Security*, *12*(1), 45–61.

Azis, M., & Santiago, F. (2024a). Transformation of consumer protection against loss of customer funds in digital banking. *Journal of Computer Science*, *3*(12).

Azis, M., & Santiago, L. (2024b). Perceived usefulness, trust, and digital literacy in the adoption of e-banking. *Asian Journal of Information Systems*, *13*(2), 65–80.

Bălănuță, A. M., Ionescu, A., & Dragomir, C. (2025). Digital literacy and ethical awareness in the era of cyber risk. *Journal of Digital Competence*, *9*(1), 21–39. https://doi.org/10.2458/jdc.v9i1.2025

Bukovec, M., & Antoliš, M. (2024). Education level as a predictor of digital risk perception and security behavior in online banking. *European Journal of Information Systems Research*, *18*(2), 155–171.

Candra, N., Mochtar, D. A., & Indrayanti, K. W. (2024). Banking customer data security protection in the era of financial technology in Indonesia. *EAS Journal of Humanities and Cultural Studies*, *6*(3), 117–122.

Candra, Y., Prasetyo, H., & Mulyono, A. (2024). Evaluasi efektivitas kampanye literasi digital pada sektor perbankan daerah. *Jurnal Ekonomi Digital Indonesia*, *4*(2), 144–160.

Cele, N., & Kwenda, F. (2024). Digital financial inclusion and user protection behavior in African banking systems. *African Journal of Economic and Management Studies*, *15*(2), 201–218.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3 (ed.)). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*, *13*(3), 319–339. https://doi.org/10.2307/249008

Dawodu, A., Balogun, M., & Bello, R. (2023a). Experiential learning and risk awareness training in strengthening digital resilience of financial institutions. *International Journal of Information Management Studies*, *9*(3), 78–94.

Dawodu, A., Balogun, M., & Bello, R. (2023b). Sequential explanatory mixed-methods in fintech adoption studies: Bridging numbers and narratives. *International Journal of Research Methodology in Business Studies*, *9*(3), 78–94.

Dewmini, W., Wijekumara, D., & Kusal, R. (2023). Digital financial literacy on financial behaviour among university students in Sri Lanka. *International Journal of Financial Studies*.

Dondokambey, M., Mandey, S., & Tumewu, F. (2023). Cybersecurity behavior among digital banking users: An application of the Protection Motivation Theory (PMT). *Jurnal Teknologi Informasi Dan Keamanan Siber*, *8*(2), 132–148.

Dondokambey, V. A., Tambariki, C., Sondakh, O. B., & Hendriana, E. (2023). Understanding Cybersecurity Behavior in the Banking Industry Using Protection Motivation Theory. *Global Conference on Business and Social Sciences*. https://doi.org/10.35609/gcbssproceeding.2023.1(31)

Eprianti, N., Srisilawati, P., Ibrahim, M. A., & M, I. M. (2024). The urgency of financial technology literacy for the community. *Social Science*. https://doi.org/10.18502/kss.v9i24.16820

Faisal, F., & Zuliarti, W. O. (2024). The Awareness Gap in Personal Data Privacy in Indonesia's Cyberspace. *International Journal of Social Science and Human Research*. https://doi.org/10.47191/ijsshr/v7-i07-84

Fitriyanti, E., & Setiorini, L. (2024). Kolaborasi lintas lembaga dalam memperkuat edukasi literasi digital di sektor keuangan Indonesia. *Jurnal Inovasi Ekonomi Dan Teknologi*, *3*(2), 89–104.

Gupta, P., & Panda, R. (2023). Digital literacy as a determinant of trust and security perception in emerging banking systems. *Journal of Financial Technology and Digital Inclusion*, *7*(2), 122–

140. https://doi.org/10.1016/j.jftdi.2023.02.007
Gusti, R., & Hilda, N. (2023). Enhancing digital literacy through QR-based technology in Indonesian banking systems. *Journal of Fintech Literacy Studies*, *2*(3), 56–72.
Handoyo, B., & Bahri, R. S. (2024). Pengaruh persepsi kemudahan, kegunaan, risiko dan fitur spesifik terhadap loyalitas nasabah pengguna mobile banking. *Jurnal Ekonomi, Manajemen Dan Sistem Informasi*, *6*(2), 1153–1166.
Handoyo, P., & Bahri, A. (2024). Literasi digital dan perilaku aman dalam transaksi keuangan daring masyarakat daerah. *Jurnal Keamanan Siber Dan Informasi*, *3*(1), 55–70.
Hariri, M., Wong, K. Y., & Abdullah, Z. (2023). Sequential explanatory research design: Integrating quantitative and qualitative insights in technology adoption studies. *Journal of Mixed Methods Research*, *17*(1), 45–62.
Hussain, S., Alam, M., & Park, J. (2023). Human factor vulnerabilities in financial cybersecurity systems. *International Journal of Information Security*, *22*(5), 415–430.
Johri, A., & Kumar, V. (2023). Cybersecurity awareness and trust in digital banking during global transformation. *Journal of Financial Innovation and Technology*, *10*(3), 225–240.
Kassar, T. (2023). Integrating Protection Motivation Theory (PMT) and Dynamic Capabilities Theory (DCT) for organizational cyber resilience. *Journal of Strategic Information Systems*, *32*(1), 101713. https://doi.org/10.1016/j.jsis.2023.101713
Khan, S., & Muhammad, A. (2022). Cybersecurity awareness and personal data protection behaviour in digital banking: A Pakistan study. *Information & Computer Security*, *30*(4), 501–519. https://doi.org/10.1108/ICS-04-2021-0053
Krishnan, R., Lee, K., & Ahmad, Z. (2023). Cybersecurity training and human error reduction in Malaysian banking institutions. *Computers & Security*, *126*, 103094. https://doi.org/10.1016/j.cose.2023.103094
Kumar, A., Sharma, S., & Patel, N. (2023). A bibliometric analysis of digital literacy and cybersecurity trust in financial technology research. *Information Systems Frontiers*, *25*(3), 675–692. https://doi.org/10.1007/s10796-023-10412-6
Kurniawan, A., & Jesica, M. (2024). Reputation, trust, and digital banking adoption among young consumers in Indonesia. *International Journal of Bank Marketing*, *42*(1), 77–95.
Lee, J. (2024). Analysis of the impact of digital literacy on life satisfaction in Korea: A polynomial regression approach. *Telematics and Informatics*, *90*, 102050.
Lee, J., & Lee, H. (2020). The effects of digital literacy and perceived security on user intention in online banking services. *Telematics and Informatics*, *51*, 101408. https://doi.org/10.1016/j.tele.2020.101408
Limna, P., & Kraiwanit, C. (2023). Cyber awareness and data protection behavior in mobile banking users. *Computers in Human Behavior Reports*, *10*, 100274. https://doi.org/10.1016/j.chbr.2023.100274
Maphosa, L. (2023). Bridging the gap between digital knowledge and protective behavior: Insights from digital literacy training programs. *African Journal of Information and Communication Technology*, *15*(1), 45–60.
Masruroh, N., Rachman, T., & Yusuf, D. (2024). Peran literasi digital dalam mencegah penipuan online di sektor perbankan. *Jurnal Sosial Teknologi Digital*, *7*(1), 32–47.
Matlala, P. (2023). Experiential awareness and cyber threat perception among digital banking users in South Africa. *African Journal of Cybersecurity and Digital Behavior*, *6*(1), 87–103.
Mbogo, C. (2024). Gamification in financial literacy education: Enhancing digital banking security awareness in developing nations. *International Journal of Digital Learning and Innovation*, *9*(1), 85–101.
Metibemu, O. (2025). Experiential cybersecurity education and its impact on digital banking trust. *Journal of Information Security and Technology Management*, *11*(1), 34–52.
Mnkandla, E., & Volk, T. (2025). Community-based gamified education as a bridge for digital literacy inequality. *Digital Education Review*, *15*(2), 102–121.
Moravec, P., Hynek, N., & Novák, R. (2024). Everyday artificial intelligence unveiled: Societal implications of digital literacy in the Czech Republic. *Technology in Society*, *80*, 102547.
Muzayyin, M., & Handayani, T. (2023). The effect of digital literacy on the risks of children dropping out of school during the COVID-19 pandemic. *Indonesian Journal of Educational Technology*.
Nagari, D., & Raharja, A. (2025). Cyber risk perception and protection motivation among digital banking users in Indonesia. *Jurnal Keamanan Informasi Dan Teknologi*, *4*(1), 88–104.

Ngiam, C., Yee, Y., & Tan, L. (2022). Building digital literacy in older adults of low income: Lessons from Project Wire Up. *Computers in Human Behavior Reports*, *7*, 100233.

Novitasari, D., Santoso, A., & Permana, I. (2020). Pentingnya pembiasaan literasi digital dalam membentuk perilaku protektif masyarakat digital Indonesia. *Jurnal Literasi Dan Pendidikan Teknologi*, *4*(1), 66–80.

O'Brien, L., Smith, K., & Tran, J. (2022). Digital divide and participation gaps in secure technology adoption. *Government Information Quarterly*, *39*(4), 101789. https://doi.org/10.1016/j.giq.2022.101789

Ogunola, A. A., Khan, S., & Yoon, J. (2024). Human error and behavioral risk in cybersecurity for digital financial services. *Computers & Security*, *130*, 103417. https://doi.org/10.1016/j.cose.2024.103417

Ogunola, A. A., Sonubi, T., Toromade, R. O., Ajayi, O. O., & Maduakor, A. H. (2024). The intersection of digital safety and financial literacy: mitigating financial risks in the digital economy. *International Journal of Research Archives*, *13*, 673–691. https://doi.org/10.30574/ijsra.2024.13.2.2183

Ogunola, A., & al., et. (2024). Digital literacy and cybersecurity awareness among financial service users. *Computing Research Journal*, *4*(2), 41–59.

Onunka, C., Ibrahim, U., & Adewale, R. (2023). Regulatory and organizational synergy in ensuring digital financial security: A global perspective. *Global Journal of Information Systems Policy*, *5*(2), 112–127.

Othman, R., Mohamad, S., & Abdullah, M. (2020). Sequential explanatory design in social science research: Applications and methodological insights. *Asian Social Science Review*, *10*(1), 25–40.

Oyewole, S., Abiola, M., & Ojo, T. (2024). Artificial intelligence and multi-factor authentication in strengthening financial data protection. *International Journal of Cybersecurity and Intelligence Studies*, *14*(1), 22–41.

Prabawa, R., Nugroho, W., & Listiani, P. (2023). Hubungan antara literasi digital dan risiko keamanan transaksi perbankan online di Indonesia Timur. *Jurnal Ekonomi Regional Dan Digital*, *5*(2), 99–113.

Pradhan, R. (2024). Financial and digital literacy as key drivers of mobile banking adoption in emerging regions. *Journal of Financial Inclusion Studies*, *8*(1), 121–137.

Puteri, A. M., Inanda, I., & Prasetio, R. B. (2024). Pengaruh literasi keuangan dan literasi digital terhadap preferensi Bank digital di kalangan mahasiswa. *Jurnal Publikasi Ilmu Manajemen*, *3*, 16–25. https://doi.org/10.55606/jupiman.v3i4.4467

Puteri, S., Fauzan, A., & Rahman, I. (2024). Analisis literasi digital dan persepsi risiko pada pengguna layanan mobile banking di Indonesia. *Jurnal Teknologi Dan Masyarakat Digital*, *4*(1), 73–88.

Rahi, S. (2023). Technology acceptance and protection motivation integration: A new model for digital financial services. *Information Systems Frontiers*, *25*(2), 335–351. https://doi.org/10.1007/s10796-023-10392-4

Repi, P. A., & Nasution, M. I. P. (2024). Menguasai literasi teknologi untuk mengatasi risiko keamanan cyber. *Jurnal Pengabdian Masyarakat*, *4*. https://doi.org/10.47467/elmujtama.v4i4.3583

Rodríguez-Pérez, J., González, F., & Martínez, L. (2021). Determinants of mobile banking adoption: The role of trust, perceived ease of use, and security perception. *Electronic Commerce Research and Applications*, *47*, 101046. https://doi.org/10.1016/j.elerap.2021.101046

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation BT - Social Psychophysiology* (pp. 153–176).

Rohendi, A., & Kharisma, D. B. (2024). Personal Data Protection in Fintech: A Case Study from Indonesia. *Journal of Infrastructure, Policy and Development*. https://doi.org/10.24294/jipd.v8i7.4158

Sabila, A., & Hasnawati, N. (2024). Perceived usefulness and ease of use in the adoption of mobile banking: An extension of TAM in Indonesia. *Jurnal Teknologi Keuangan Digital*, *5*(1), 50–66.

Savitha, R., Kumar, P., & Menon, S. (2023). Gamified digital literacy education for cybersecurity awareness: An empirical study. *Computers in Human Behavior Reports*, *10*, 100256. https://doi.org/10.1016/j.chbr.2023.100256

Sebayang, F., Rachman, H., & Siregar, P. (2023). Determinants of behavioral intention to use

mobile banking in Indonesia. *Journal of Behavioral Economics and Digital Finance*, *11*(3), 212–231.

Sebayang, F., Rachman, H., & Siregar, P. (2024). Innovative education strategies for improving digital trust and literacy in financial institutions. *Jurnal Pendidikan Digital Dan Inklusi Keuangan*, *5*(2), 95–110.

Shaikh, A., Tan, C., & Lim, P. (2023). AI-based anomaly detection for secure financial transactions. *Journal of Applied Cybersecurity*, *5*(2), 101–120.

Simatupang, D., Raharjo, B., & Setiawan, Y. (2024). Analisis efektivitas sosialisasi keamanan digital pada lembaga keuangan daerah. *Jurnal Komunikasi Digital*, *2*(4), 56–70.

Sitriani, R., & Zainuddin, M. (2025). The influence of financial literacy and digital literacy on MSME profitability in Indonesia. *Journal of Economics and Digital Business*.

Susilawati, N., Prabowo, D., & Handayani, S. (2024). Transformasi digital berkelanjutan dan keamanan data dalam sektor perbankan daerah. *Jurnal Transformasi Ekonomi Digital Indonesia*, *6*(1), 67–83.

Sytnyk, I., & Polovchak, O. (2024). Cybersecurity and digital transformation in modern banking systems. *Journal of Financial Technology and Security*, *9*(1), 50–68.

Utami, E. Y., Puteri, L. D., & Susilawati, M. (2025). Digital literacy education and user protection in regional banking systems. *Asian Journal of Banking and Finance*, *6*(1), 55–72.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2019). Unified theory of acceptance and use of technology: A refinement and extension of the TAM model. *MIS Quarterly*, *43*(1), 293–315. https://doi.org/10.25300/MISQ/2019/14118

Wakoli, P. (2024). Organizational commitment and cybersecurity compliance in digital banking institutions. *African Journal of Banking and Finance*, *12*(3), 174–189.

Widarwati, R., Nugraha, D., & Amalia, F. (2022). Peran literasi digital terhadap inklusi keuangan masyarakat di era perbankan digital. *Jurnal Ekonomi Dan Keuangan Digital*, *5*(4), 211–225.

Zahiroh, S. (2020). Cybersecurity readiness and digital skills for banking digitalization in Indonesia. *Jurnal Transformasi Digital Indonesia*, *2*(2), 78–93.

Zakirova, L., & Pol, A. (2024). Digital literacy gaps and data security risks in financial institutions. *Information Systems and Society*, *12*(2), 180–197.

Zaman, S., & Khalid, R. (2025). Trust, social influence, and perceived ease of use in Islamic digital banking adoption. *South Asian Journal of Financial Innovation*, *6*(1), 43–59.